



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,980	12/30/2003	Jon C. Graff	042933/272520	8836
826	7590	07/17/2007	EXAMINER	
ALSTON & BIRD LLP			WANG, HARRIS C	
BANK OF AMERICA PLAZA			ART UNIT	
101 SOUTH TRYON STREET, SUITE 4000			PAPER NUMBER	
CHARLOTTE, NC 28280-4000			2139	
			MAIL DATE	DELIVERY MODE
			07/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/748,980

Applicant(s)

GRAFF, JON C.

Examiner

Harris C. Wang

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 April 2007.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2139

DETAILED ACTION

1. Claims 1-18 are amended

Claims 19-26 are new

Response to Amendment

Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 6-9, 12-15, 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Juitt (20030087629) in view of Ludwig (7222107).

Regarding Claims 1, 7, 19 and 23

Juitt teaches a system comprising:

a terminal configured to communicate at least one of within and across at least one network, wherein the terminal is included within an organization including a plurality of terminals, each terminal being at at least one of a plurality of positions within the organization; (*"The mobile device 100 can be any sort of device that has wireless communication capability, including...telephones" Paragraph [0037]*). The Examiner interprets the telephone as the terminal. The wireless telephone is shown as capable of communicating within and across at least one network as shown in Fig. 1 (Mobile Device 100 communicates with Wireless Network 105, where according to the background of the invention Juitt writes that "Wireless networks typically include mobile devices" Paragraph [0003]).

a primary certification authority (CA) configured to provide an identity certificate to the terminal, wherein the primary CA is configured to issue an identity certificate to each terminal of the organization; *In Paragraph [0011] Juitt writes "the request [to access a protected network] might be an explicit request for access and can include an identifier and authentication information (e.g. a...digital certificate). The Examiner interprets a digital certificate that provides identifier information as an identity certificate. It is inherent that a CA is needed to distribute Identity Certificates.*

a secondary CA capable of providing at least one role certificate to the terminal based upon the at least one position of the terminal within the organization, wherein the organization includes a plurality of secondary CA's configured to issue at least one role certificate to respective groups of terminals of the organization based upon the at least one position of each of the respective terminals within the organization; (*"In one*

Art Unit: 2139

embodiment, a role definer in the gateway server defines roles and assigns them to users. The role definer can specify network resources and degree of access to the protected network...Access privileges can be differentiated for authorized users based on roles."

[Paragraph [0020]] The Examiner interprets the role assigner as the secondary CA capable of issuing role certificates based on the position of the respective terminals within the organization. An example of Juitt assigning roles based on position is also found in Paragraph [0020] where "an 'engineer' role can be defined with full access to engineering department servers, but limited access to finance department servers."

and a server configured to authenticate the terminal based upon the identity certificate and the at least one role certificate of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server. (*"Once the user is authenticated and assigned a role, an access controller in the gateway server provides access to the protected network based on the assigned role"* Paragraph [0021], Fig. 1A Authentication Server 125). The Examiner interprets the authentication process is done using an identity digital certificate as described above. It is inherent that a server has at least one processor.

Juitt however does not explicitly say that the role assigner is configured to assign roles using a role certificate.

Ludwig teaches a method for role-based authorization, where "a role certificate plays an important role in the method. It is assumed that within any company C there exists a set of well-defined roles...and that each user U in the company C is assigned one or several roles" (Column 7, lines 14-18). Ludwig further teaches "If U has several roles then there will be a role certificate for each role. It is important to note that each

Art Unit: 2139

role certificate has a public and corresponding private key so that users may produce signatures in their role capacities. Thus each user will have at least two certificates, a standard X.509v3 certificate CertCA(U) that binds their name to a public key , and then an anonymous role certificate (CertCA(U,R) that binds their role to a public key.”

Column 7 lines 56-63).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the role assigner of Juitt to assign roles using role certificates for the purpose of authentication.

The motivation is that using role certificates to assign roles is very well known in the art of Role-Based Access control.

The Examiner notes that the assigned roles as taught by Juitt do in fact authenticate in a manner consistent with what the Applicant describes in their own specification. In Paragraph [0054] of the Applicant's specification, the Applicant writes “the secondary CA can bind the identity of the terminal with the position of the terminal.” So essentially, before a role can be assigned, first the identity of the user must be known because a user can have only one identity certificate but many role certificates. In other words, you cannot authenticate a user's identity solely by the role certificate, because there are many users for each role.

Therefore the Examiner, in the First Office Action, interpreted the ID certificate as authenticating and the role certificate as the certificate that determined whether to grant the terminal access to resources based on the way the claim was structured. However, in the broadest sense one can still interpret authentication using the assigned role as to

Art Unit: 2139

proving the identity of the user belonging to the role, which is provided when the role is assigned.

Claims 7 and 19 describe the method associated with the system of Claim 1 and is taught by the cited art.

Claim 23 describes the server which is taught in the cited art above.

Regarding Claims 2 –3, 8-9, 20-21

Juitt and Ludwig teach the system according to claim 1, wherein the terminal comprises a terminal included within an organization comprising a cellular network.

("The wireless network 105 can support a wide variety of wireless networks, including cellular networks" Paragraph [0038])

Juitt and Ludwig do not explicitly teach that each terminal being at one of a plurality of positions comprising a plurality of service plans offered by the cellular network operator. Where the terminal is in a customer base of a cellular service provider that includes a plurality of terminals.

It would have been obvious to one of ordinary skill in the art at the time of the invention to include cellular service plans as the roles assigned to mobile devices in the system taught by Juitt.

The motivations is first that it is very well known that cellular networks are used by cellular service providers, and that cellular service providers offer different cellular service plans. Because roles are defined as groups of users that have certain access

Art Unit: 2139

privileges, and cellular service providers contain groups of subscribers different access privileges, based on their service plans, it is clear that a service plan can be considered as a role.

Claims 8-9 and 20-21 describes the method associated with the system of Claims 2-3 and is taught by the cited art.

The Examiner notes that Christoffel (US20020136226) which is incorporated by reference to Juitt (both references share the same inventors) further elaborates on the nature of the system with more emphasis given to the mobile device as a cellular phone and the network as a cellular network. The Examiner would like to point out in particular Paragraph [102] where Christoffel writes "the authentication server tells the gateway server which network group the mobile device "belongs to." So, for example, if the user is a customer of GPRS cellular operator who is temporarily using a WISP, then the domain would be the network system of the cellular operator."

Regarding Claim 6, 12

Juitt and Ludwig teach a system according to claim 1, wherein the terminal is capable of requesting access to at least one resource of a server before the server authenticates the terminal, and wherein the server is capable of granting access to the at least one resource if the terminal is authenticated. (*"The gateway server 120 authenticates the mobile device 100 utilizing its authentication subsystem 155, which may*

include authenticating the device or the user or owner of the device using an authentication server 125...the authentication server...determines whether the mobile device is authorized as well...thus the mobile device can be authorized to initiate a session with the protected network 110 via the wireless network 105 based on the access privilege information provided by the authentication server 125." Paragraph [0056])

Claim 12 is the method associated with the system described in Claim 6, and is taught by the cited art.

Regarding Claim 13,

Juitt teaches a terminal included within an organization including a plurality of terminals, each terminal being at at least one of a plurality of positions within the organization (*Fig. 1 shows the Mobile Device 100, further described in Paragraph [0037] as a telephone that "has wireless capability" and the wireless network 105 described in Paragraph [0038] as a cellular network. It is inherent that a cellular phone will have a controller and a memory*).

Juitt teaches that the mobile device is configured to communicate at least one of within and across at least one network, wherein the mobile device is configured to obtain an identity certificate from a primary certification authority (CA) configured to issue an identity certificate to each terminal of the organization. (*"The request...can include identifier and authentication information (e.g. a digital certificate)"*)

Juitt further teaches wherein the mobile device is also configured to obtain at least one role. (*"In one embodiment, a role definer in the gateway server defines roles and*

assigns them to users. The role definer can specify network resources and degree of access to the protected network...Access privileges can be differentiated for authorized users based on roles." [Paragraph [0020]]

and the mobile device is then configured to store the identity certificate and at least one role (*"authenticating the mobile device is understood to include any one or a combination of suitable authentication techniques...Examples of authentication information include...digital certificate"* Paragraph [0016]) (*"a role definer in the gateway server defines roles and assigns them to users"* Paragraph [0020]), It is inherent that the mobile device requires memory for storing identity certificates and roles.

Juitt further teaches wherein the mobile device is also configured to communicating with a server such that the server is configured to authenticate the terminal based upon the identity certificate and the at least one role of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server. (*Figure 1A, Authentication Server*)

Juitt does not explicitly teach where the mobile device is assigned a role certificate from a secondary CA based upon the at least one position of the terminal within the organization.

Ludwig teaches a method for role-based authorization, where "a role certificate plays an important role in the method. It is assumed that within any company C there exists a set of well-defined roles...and that each user U in the company C is assigned

Art Unit: 2139

one or several roles" (*Column 7, lines 14-18*). Ludwig further teaches "If U has several roles then there will be a role certificate for each role. It is important to note that each role certificate has a public and corresponding private key so that users may produce signatures in their role capacities. Thus each user will have at least two certificates, a standard X.509v3 certificate CertCA(U) that binds their name to a public key , and then an anonymous role certificate (CertCA(U,R) that binds their role to a public key."

Column 7 lines 56-63).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the role assigner of Juitt to assign roles using role certificates for the purpose of authentication.

The motivation is that using role certificates to assign roles is very well known in the art of Role-Based Access control.

Regarding Claims 14-15, 24-25

Juitt and Ludwig teach a terminal according to claim 13, and a server for communicating with the terminal in Claim 23.

Juitt and Ludwig do not explicitly teach that each terminal being at one of a plurality of positions comprising a plurality of service plans offered by the cellular network operator. Where the terminal is in a customer base of a cellular service provider that includes a plurality of terminals.

It would have been obvious to one of ordinary skill in the art at the time of the invention to include cellular service plans as the roles assigned to mobile devices in the system taught by Juitt.

The motivations is first that it is very well known that cellular networks are used by cellular service providers, and that cellular service providers offer different cellular service plans. Because roles are defined as groups of users that have certain access privileges, and cellular service providers contain groups of subscribers different access privileges, based on their service plans, it is clear that a service plan can be considered as a role.

Regarding Claim 18,

Juitt and Ludwig teach a terminal according to claim 13, wherein the controller is configured to requesting access to at least one resource of a server before the server authenticates the terminal such that the server is configured to granting access to the at least one resource if the terminal is authenticated. (*"The gateway server 120 authenticates the mobile device 100 utilizing its authentication subsystem 155, which may include authenticating the device or the user or owner of the device using an authentication server 125...the authentication server...determines whether the mobile device is authorized as well...thus the mobile device can be authorized to initiate a session with the protected network 110 via the wireless network 105 based on the access privilege information provided by the authentication server 125."* Paragraph [0056])

Claims 4-5 and 10-11, 16-17, 22, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Juitt and Ludwig in view of the Technical Report Number 558 "A role and context based security model" by Yolanta Beresnevichiene pgs. 76-80 (Hereafter referred to as "the Technical Report")

Regarding Claims 4, 10, 16, 22, 26

Juitt and Ludwig teach the system according to claim 1, and the method according to claim 7, and the terminal according to claim 13, and the server according to claim 23, wherein the secondary CA is capable of providing at least one role certificate. Juitt does not teach having an associated validity time no greater than a validity time of the identity certificate provided by the primary CA.

The Technical Report teaches in Section 7.6.2 Life-Time (pg. 78) that "the validity of role certificates could be almost as long as of identity certificates."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Juitt with a role certificate with a shorter validity time than the identity certificate.

The motivation to combine is that a role may change more frequently whereas an identity should last longer. Therefore the role certificate should have a shorter validity time than an identity certificate.

Art Unit: 2139

Claims 10 and 22 describes the method associated with the system of Claim 4 and is taught by the cited art.

Regarding Claim 5, 11, 17

Juitt, Ludwig and the Technical Report teach a system according to claim 4, and the method according to claim 10, and the terminal according to claim 16. The combined references do not explicitly teach that the server is capable of authenticating the terminal based upon the validity times of the identity certificate and at least one role certificate of the respective terminal.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the authentication system described in Claim 4 to further include the limitation of validity time.

The motivation to modify is to provide an extra layer of access control.

Claim 11 describes the method associated with the system of Claim 5 and is taught by the cited art.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

Art Unit: 2139

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW


TAGHI ARANI
PRIM
6/29/04